Office for
Civil Rights

Making a List and Checking it Twice: HIPAA and IT Asset Inventories

Office for Civil Rights
Cybersecurity Newsletter 2020
12/8/20

HIPAA and IT Asset Inventories

The HIPAA Security Rule requires covered entities and business associates to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that it creates, receives, maintains, or transmits.1 Conducting a risk analysis, which is an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI held by an organization, is not only a Security Rule requirement,2 but also is fundamental to identifying and implementing safeguards that comply with and carry out the Security Rule standards and implementation specifications.3 However, despite this long-standing HIPAA requirement, OCR investigations frequently find that organizations lack sufficient understanding of where all of the ePHI entrusted to their care is located. Although the Security Rule does not require it, creating and maintaining an up-to-date, information technology (IT) asset inventory could be a useful tool in assisting in the development of a comprehensive, enterprise-wide risk analysis, to help organizations understand all of the places that ePHI may be stored within their environment, and improve their HIPAA Security Rule compliance.

Creating an IT Asset Inventory

Generally, an enterprise-wide IT asset inventory is a comprehensive listing of an organization's IT assets with corresponding descriptive information, such as data regarding identification of the asset (e.g., vendor, asset type, asset name/number), version of the asset (e.g., application or OS version), and asset assignment (e.g., person accountable for the asset, location of the asset).

The HHS Security Risk Assessment Tool includes inventory capabilities that allow for manual entry or bulk loading of asset information with respect to ePHI. Larger, more complex organizations may choose dedicated IT Asset Management (ITAM) solutions that include automated discovery and update processes for asset and inventory management. HIPAA covered entities and business associates using the NIST Cybersecurity Framework (NCF)4 should be able to leverage the inventory components of the NCF's Asset Management (ID.AM) category, which includes inventorying hardware (ID.AM-1), inventorying software (ID.AM-2), and mapping communication and data flows (ID.AM-3), to assist in creating and maintaining an IT asset inventory that can be used in and with their Security Rule risk analysis process with respect to ePHI. When creating an IT asset inventory, organizations can include:

- Hardware assets that comprise physical elements, including electronic devices and media, which make up an organization's networks and systems. This can include mobile devices, servers, peripherals, workstations, removable media, firewalls, and routers.

- Software assets that are programs and applications that run on an organization's electronic devices. Well-known software assets include anti-malware tools, operating systems, databases, email, administrative and financial records systems, and electronic medical/health record systems. Though lesser known, there are other programs important to IT operations and security such as backup solutions, virtual machine managers/hypervisors, and other administrative tools that should be included in an organization's inventory.

- Data assets that include ePHI that an organization creates, receives, maintains, or transmits on its network, electronic devices, and media. How ePHI is used and flows through an organization is important to consider as an organization conducts its risk analysis.5

How an IT Asset Inventory Can Help Improve an Organization's Risk Analysis

HIPAA covered entities and business associates are required to conduct an accurate and thorough assessment of the risks to the ePHI it maintains. Identifying, assessing, and managing risk can be difficult, especially in organizations that have a large, complex technology footprint. Understanding one's environment – particularly how ePHI is created and enters an organization, how ePHI flows through an organization, and how ePHI leaves an organization – is crucial to understanding the risks ePHI is exposed to throughout one's organization.

When creating or maintaining an IT asset inventory that can aid in identifying risks to ePHI, it may be beneficial to consider other IT assets that may not store or process ePHI. An entity's risk analysis obligation is to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentially, integrity, and availability of ePHI held by the covered entity or business associate."6 Assets within an organization that do not directly store or process ePHI may still present a method for intrusion into the IT system, that could lead to risks to the confidentiality, integrity, and availability of an organization's ePHI. For example, consider an Internet of Things (IoT) or a smart, connected device that provides access to facilities for maintenance personnel for control and monitoring of an organization's heating, ventilation, and air conditioning (HVAC). Although it does not store or process ePHI, such a device can present serious risks to sensitive patient data in an organization's network. Unpatched IoT devices with known vulnerabilities, such as weak or unchanged default passwords installed in a network without firewalls, network segmentation, or other techniques to deny or impede an intruder's lateral movement, can provide an intruder with a foothold into an organization's IT network. The intruder may then leverage this foothold to conduct reconnaissance and further penetrate an organization's network and potentially compromise ePHI.

Real world examples of IoT devices used for malicious activities include incidents reported by Microsoft in which malicious actors were able to compromise a VOIP phone, printer, and video decoder to gain access to corporate networks. The hackers were able to exploit unchanged default passwords and unpatched security vulnerabilities to compromise these devices. Once inside the network, the hackers were able to conduct reconnaissance and access other devices on the corporate network in search of additional privileges and high-value data.7

An IT asset inventory that includes IoT devices can strengthen an organization's risk analysis by raising awareness of the potential risks such devices may pose to ePHI. The lack of an inventory, or an inventory lacking sufficient information, can lead to gaps in an organization's recognition and mitigation of risks to the organization's ePHI. Having a complete understanding of one's environment is key to minimizing these gaps and may help ensure that a risk analysis is accurate and thorough, as required by the Security Rule.

Ongoing Process and Benefits

An IT asset inventory can aid in an organization's overall cybersecurity posture and HIPAA compliance in other ways, too. For example, HIPAA covered entities and business associates must "[i]mplement policies and procedures that govern the receipt and removal of hardware and electronic media that contain [ePHI] into and out of a facility, and the movement of these items within the facility."8 This includes servers, workstations, mobile devices, laptops, and any other hardware or media that contains ePHI. Receipt, removal, and movements of such devices can be tracked as part of an organization's inventory process. This has become more important as organizations' networks and enterprises grow increasingly large and complex – especially, considering the proliferation and use of mobile devices and removable media by the workforce. If reasonable and appropriate, organizations also may consider adding location and owner or assignment information to an IT asset inventory to assist in an organization's ability to "[m]aintain a record of the movements of hardware and electronic media and any person responsible . . . ."9

Further, by comparing its inventory of known IT assets against the results of network scanning discovery and mapping processes, an organization can identify unknown or "rogue" devices or applications operating on its network. Once identified, these previously unknown devices can be added to the inventory and the risks they may pose to ePHI identified, assessed, and mitigated. An inventory can also be integral to an organization's vulnerability management program. New software bugs and vulnerabilities are identified on a regular basis. Subsequently, software updates and patches are regularly issued to fix these bugs and mitigate these vulnerabilities. An enterprise-wide IT asset inventory can help an organization identify and track affected devices to facilitate and verify timely application of updates and patches.

Additional Resources:

NIST SP 800-66 Rev. 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule:

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf

HHS Security Risk Assessment Tool:

- https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

August 2018 Cyber Security Newsletter: Considerations for Securing Electronic Media and Devices:

- https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-august-2018-device-and-media-controls.pdf

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks:

- https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

NIST SP 1800-5: IT Asset Management:

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf

** This document is not a final agency action, does not legally bind persons or entities outside the Federal government, and may be rescinded or modified in the Department's discretion.*

Footnotes

1. See Security Standards: General Rules, 45 CFR 164.306; Administrative Safeguards, 45 CFR 164.308; Physical Safeguards, 45 CFR 164.310; and Technical Safeguards, 45 CFR 164.312.

2. See Risk Analysis, 45 CFR 164.308(a)(1)(ii)(A).

3. See Maintenance, 45 CFR 164.306(e); Evaluation, 45 CFR 164.308(a)(8); Device and Media Controls, 45 CFR 164.310(d)(1); and Documentation Updates, 45 CFR 164.316(b)(2)(iii).

4. https://www.nist.gov/cyberframework.

5. "The analysis of data flows and data uses that covered entities are doing so as to comply with the Privacy Rule should also serve as the starting point for parallel analysis required by [the Security Rule]," Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334, 8371 (February 20, 2003).

6. See 45 CFR 164.308(a)(1)(ii)(A), Risk Analysis (emphasis added).

7. https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

8. 45 CFR 164.310(d)(1), Device and Media Controls.

9. 45 CFR 164.310(d)(2)(iii), Accountability (Addressable).